REMARKS

Claims 1, 2, and 4-20 are currently pending. The Examiner has rejected Claims 12 and 17 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Additionally, the Examiner has rejected claims 12, 14, and 16 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,775,779 to England et al. The Examiner has also rejected claims 1, 2, 4-11, 13, 15, and 17-20 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose. The following remarks are considered by Applicants to overcome each of the Examiner's outstanding rejections. An early Notice of Allowance is therefore requested.

I. Summary of Relevant Law

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. The determination of obviousness rests on whether the claimed invention as a whole would have been obvious to a person of ordinary skill in the art at the time the invention was made. In determining obviousness, four factors should be weighed: (1) the scope and content of the prior art, (2) the differences between the art and the claims at issue, (3) the level of ordinary skill in the art, and (4) whatever objective evidence may be present. Obviousness may not be established using hindsight or in view of the teachings or suggestions of the inventor. The Examiner carries the burden under 35 U.S.C. § 103 to establish a prima facie case of obviousness and must show that the references relied on teach or suggest all of the limitations of the claims.

II. REJECTION OF CLAIMS 12 AND 17 UNDER 35 U.S.C. § 112, FIRST PARAGRAPH

Examiner contends that claims 12 and 17 added material that is not supported by the original disclosure, namely that the operating system is approved to be loaded on that specific computer platform alone. Office Action (8/17/05), P. 2-3. Claims 12 and 17 both require "...that said operating system is approved to be loaded on that specific computer platform alone." Contrary to the Examiner's contention, this is taught by the original specification.

The specification describes at least two methods of ensuring security: (1) use of public/private signature (figs. 2-3) and (2) the use of encryption keys (figs. 4-7). While explaining (2), the specification states that "[s]imilar to the public/private signature keys, the public encryption key is distinctively related to a private decryption key," and that "both encryption/decryption keys are **unique to a particular computer platform** rather than a particular programmer." Application, P. 9, Lns. 8-11. This language creates the direct support for the claim language that the Examiner contends is not supported.

The fact that this language is described when using application programs and object files as the illustrative example instead of O/S does not make this claim language new matter. The description of method (2) was not limited to application programs and object files. The application makes it clear that these two methods are equally applicable to O/S, application programs and object files. See Application, p. 6, lines 20-22 and P. 8, Lns. 16-20. Since O/S, application programs and object files are all software code, the applicability of these methods to these objects would be understood by one of skill in the art.

This general applicability is also demonstrated when the applicant describes an alternative embodiment involving sending public signatures to the manufacturers. See page 12, lines 16- page 13, line 2. In this alternative embodiment, the application is still using application

programs and object files as the illustrative example. However, after the explanation of this alternative, the specification states that this alternative embodiment is not available to O/S verification. See page 13, lines 3-6. If the applicant did not intend that the methods (1) and (2) were not equally applicable to O/S, program applications and object files, then it would have been unnecessary to have such a disclaimer. For the Examiner to read the teaching of the specification differently is unfairly narrowing and contrary to the language in the specification.

All of the above portions of the specification of the Application support the claim limitation that "...that said operating system is approved to be loaded on that specific computer platform alone." It is therefore respectfully requested that Examiner remove the rejection of claim 12 and 17 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.

III. REJECTION OF CLAIMS 12, 14, AND 16 UNDER 35 U.S.C. § 102(E) BASED ON ENGLAND ET AL

With respect to this rejection, the Examiner contends that:

> "England discloses a computer system for content protection wherein the operating system is authenticated during the boot process before it is loaded (Col. 2, lines 16-40), which meets the limitations of a receiving platforms, each of said receiving platforms having firmware and an operating system, said firmware authenticating said operating system. **The fact that the operating system is authenticated on the computer system meets the limitation of the operating system being approved to be loaded on that specific computer platform alone.**"

Office Action (8/17/05), P. 3 (emphasis added). However, this misconstrues the teachings of England et al. Specifically, as is described in detail below, England et al never teaches a number of the recited claim limitations, including an operating system "approved to be loaded on that

specific computer platform alone." 7/18/05 Response to 3/16/05 Office Action, P. 4, Claim 12. As such Applicants respectfully asserts that the Examiner's rejection stands in error.

Claim 12

Claim 12 of the current application requires:

> "a plurality of receiving platforms, each of said receiving platforms having firmware and an operating system, said firmware authenticating said operating system, **to ensure that said operating system is approved to be loaded on that specific computer platform alone**;"

7/18/05 Response to 3/16/05 Office Action, P. 4 (emphasis added).

England et al, however, discloses that the authentication of the operating system is "to authenticate to remote distributors that the computer is running a copy of an operating system that is trusted to provide adequate protection for digital content, and that even a legitimate user in physical possession of the computer cannot vitiate this protection." England et al, Col. 2, Lns. 18-23. Such an authentication relates to the features of an operating system and whether or not it has the requisite protection capabilities. Such an authentication bears no relation to the correlation of a specific operating system to a specific computer platform. Therefore, England fails to disclose the Claim 12 limitation that the operating system is approved to be loaded on a specific computer platform alone.

Additionally, Claim 12 requires:

> "**each of said receiving platforms having: (a) a public signature identification key to authenticate said signatures** and (b) firewalls associated with said application programs and object files to control access to each of said application programs and object files,"

7/18/05 Response to 3/16/05 Office Action, P. 4 (emphasis added).

This is another claim limitation England et al fails to disclose. While England et al does disclose that applications and modules may have public keys, it never teaches that receiving platforms may have public signature identification keys. England et al, Col. 8, Lns. 42-

46. Furthermore, Examiner never contends that England et al discloses this limitation. Therefore, England et al fails to set forth this claim limitation.

Claim 12 also requires:

> "said sending station including: (a) a plurality of application programs, (b) a plurality of object files, **(c) a plurality of handler programs, each associated with a separate one of said object files, and (d) a plurality of secret key encoded signatures, each distinctive to a subset of said application programs and said object files,"**

7/18/05 Response to 3/16/05 Office Action, P. 4 (emphasis added).

England et al fails to disclose "a plurality of handler programs, each associated with a separate one of said object files." England et al does disclose a single security manager 420, however, this security manager is general to all object files and is certainly not a "plurality ... associated with a separate one of said object files." England et al, Col. 7, Ln. 57 – Col. 14, Ln. 9. Furthermore, Examiner never contends that England et al discloses this limitation. Therefore, England et al fails to set forth this claim limitation.

In addition, England et al fails to disclose "a plurality of secret key encoded signatures, each distinctive to a subset of said application programs and said object files." England et al discloses that the operating system, modules, and security manager may have a secret key. England et al, Col. 2, Lns. 37-39; Col. 10, Lns. 17-20; Col. 14, Lns. 22-25. Never does England et al disclose a plurality of secret key encoded signatures for application programs or object files. Certainly, England et al never discloses a plurality of secret key encoded signatures, **each distinctive** to a subset of application programs and object files. Furthermore, Examiner never contends that England et al discloses this limitation. Therefore, England et al fails to set forth this claim limitation.

Finally, Claim 12 requires:

> "the one of said **handler programs** associated with each of said object files permitting access to the associated object files by an appropriate one or more of said application programs.
>
> each of said **handler programs** being programmable to permit multi-parameter control over access to the associated one of said object files."

7/18/05 Response to 3/16/05 Office Action, P. 4 (emphasis added).

As discussed above, England et al fails to disclose handler programs. England et al certainly fails to teach that handler programs are programmable to permit multi-parameter control over access to the associated one of said object files." Furthermore, Examiner never contends that England et al discloses this limitation. Therefore, England et al fails to set forth this claim limitation.

For all of the foregoing reasons, England et al does not contain each and every element as set forth in Claim 12. Therefore, Applicants respectfully assert that Examiner has failed to establish a prima facie case of anticipation of independent Claim 12 and corresponding claims 14 and 16 because they are dependant from Claim 12. Therefore, Applicants respectfully request that Examiner remove the rejection of claims 12, 14, and 16 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,775,779 to England et al.

Claim 14

Claim 14 is dependent upon Claim 12. As Claim 12 is allowable, so must be Claim 14. In addition, Claim 14 specifies that "said signature identification is provided through a **signature creation algorithm** and a secret key at said sending station and through a signature verification algorithm and a **public key at each receiving platform.**" 7/18/05 Response to 3/16/05 Office Action, P. 5 (emphasis added). Examiner contends that "England discloses that the digital signature is created with a secret key (Col. 11, lines 6-17)." Office Action (8/17/05), P. 4. Applicants respectfully disagree with Examiner's assertion of England et al's disclosure.

The portion of England cited by the examiner refers to public keys and to secret information, but never to secret keys. But even if Examiner is correct, England et al teaches that it is the content provider ("CP") that has the public key and not the receiving platform. Furthermore, England et al never discloses a signature creation algorithm, and Examiner never contends otherwise. It is therefore respectfully requested that Examiner remove the rejection of Claim 14 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,775,779 to England et al.

Claim 16

Claim 16 is dependent upon Claim 12. As Claim 12 is allowable, so must be Claim 16. In addition, Claim 16 specifies that:

> "**said sending station has a plurality of secret key encoded signatures, each signature being distinctive to a separate set of application programs and data texts,**
>
> each receiving platform having a plurality of public signature identification keys to correspond to the plurality of secret keys at said sending station."

7/18/05 Response to 3/16/05 Office Action, P. 5 (emphasis added).

Examiner contends that "England discloses that the digital signature is created with a public key (Col. 9, lines 18-20), which meets the limitation of each receiving platform having a plurality of public signature identification keys to correspond to the plurality of secret keys at said sending station." Office Action (8/17/05), P. 5. Applicants respectfully disagree with Examiner's assertion of England et al's disclosure. The portion of England cited by the examiner refers to an audio player trusting an operating system component signed with a public key. Never is any correspondence of public signature identification keys to secret keys disclosed. Furthermore, England et al never discloses secret key encoded signatures distinctive to a separate set of application programs and data texts, and Examiner never contends otherwise. It is

therefore respectfully requested that Examiner remove the rejection of Claim 14 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,775,779 to England et al.

IV. REJECTION OF CLAIMS 1, 2, 4-11, 13, 15, AND 17-20 UNDER 35 U.S.C. § 103(A) BASED ON ENGLAND ET AL IN VIEW OF ROSE

With respect to this rejection, the Examiner contends that:

> "The fact that the operating system is authenticated on the computer system meets the limitation of **the operating system being approved to be loaded on that specific computer platform alone.**"

Office Action (8/17/05), P. 6.

> "The system further provides for secure encrypted sessions wherein encrypted content is transmitted (Col. 11, line 55 - Col. 12, line 5), which meets the limitation of an output interface connected to said platform to allow said platform to transmit output data out of said platform, and said output data being encrypted when transmitted."

Office Action (8/17/05), P. 6 (emphasis added). However, this misconstrues the teachings of England et al, because England et al does not disclose either an operating system approved to be loaded on a specific computer platform alone or an output interface which allows a platform to transmit output data.

Claim 1

With respect to examiner's first assertion, as discussed above, England et al discloses that the authentication of the operating system is "to authenticate to remote distributors that the computer is running a copy of an operating system that is trusted to provide adequate protection for digital content, and that even a legitimate user in physical possession of the computer cannot vitiate this protection." England et al, Col. 2, Lns. 18-23. As discussed above in relation to Claim 12, this is completely unrelated to whether or not the operating system is

approved to be loaded on a specific computer platform alone. Therefore, England et al fails to set forth this claim limitation.

Claim 1 requires:

> "wherein **said operating system decrypts** said input data with a private **decryption key unique to that specific computer platform** to ensure that said input data is authorized for access on said specific computer platform alone;"

7/18/05 Response to 3/16/05 Office Action, P. 2 (emphasis added).

Examiner asserts that "England discloses that the content is decrypted using secret keys (Col. 11, lines 6-30)..." Office Action (8/17/05), P. 7. However, Applicants respectfully disagree with Examiner's assertion of England et al's disclosure. The portion of England cited by the examiner refers to public keys and to secret information, but never to secret keys. But even if Examiner is correct, England et al teaches that it is the content provider ("CP") that accomplishes the decryption and not the operating system.

Furthermore, while Examiner admits that England et al does not disclose that the decryption key is a private decryption key unique to a specific computer platform, Examiner asserts that:

> "Rose discloses a method for try and buy application programs wherein a the programs are encrypted and transmitted to users who decrypt them with private keys that are unique to their user terminals (Col. 10, lines 43-53), which meets the limitation of said operating system decrypts said input data with a private decryption key unique to that specific computer platform to ensure that said input data is authorized for access on said specific computer platform alone."

Office Action (8/17/05), P. 7.

However, Rose makes it very clear that it is the Application Builder, and not the operating system that decrypts the encrypted Application Program. Rose, Col. 8, Lns. 11-31. Therefore, Rose fails to disclose the first portion of the above claim limitation.

In addition, Rose discloses that the private key is contained on, and unique to, the Application Builder and not on the specific computer platform. Rose, Col. 10, Lns. 43-53. The "Applications Builder's private key ... is unique for each client computer on which it is installed." *Id.* At first blush, this may seem to say that the private key is unique to the computer platform. However, this would be an inaccurate statement. As Rose states, it is the **Application Builder's** private key and not the operating platform's private key. This is also clearly displayed in Figure 1 which depicts the contents of the Application Builder. Therefore, in reality, the private key is specific to that particular copy of the Application Builder which is maintained on the computer platform. Removing the Application Builder from the platform would remove the Application Builder's corresponding private key as well.

Therefore, even when England et al and Rose are combined, they fail to set forth this claim limitation.

As such, Applicants respectfully assert that Examiner has failed to establish a prima facie case of obviousness of independent Claim 1 and corresponding claims 2, and 4-11 because they are dependant from Claim 1. Therefore, Applicants respectfully request that Examiner remove the rejection of claims 1, 2, and 4-11 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Claim 2

Claim 2 is dependent upon Claim 1. As Claim 1 is allowable, so must be Claim 2. In addition, Claim 2 specifies that "said hardware authenticates said operating system by verifying a digital signature associated with said operating system." Applicants respectfully disagrees with Examiner's assertion that "England discloses that the operating system

authentication uses digital signatures for verification (Col. 2, lines 16-40)." Office Action (8/17/05), P. 7. While England et al states that authenticating an operating system allows it to maintain secret keys and other data, nowhere does England et al disclose that the authentication of the operating system occurs by verifying a digital signature associated with that operating system. It is therefore respectfully requested that Examiner remove the rejection of Claim 2 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Claim 6

Claim 6 is dependant from Claim 4, which is in turn dependant from Claim 1. As Claim 1 is allowable, so must be Claim 6. In addition, Claim 6 specifies "a sending station capable of creating a digital signature with a secret signature key; said secret signature key being distinctively associated with said sending station." 8/18/05 Response to 3/16/05 Office Action, P. 3. Examiner contends that "England discloses that the digital signature is created with a secret key (Col. 11, lines 6-17)." Office Action (8/17/05), P. 7. Applicants respectfully disagree with Examiner's assertion of England et al's disclosure. The portion of England cited by the examiner refers to public keys and to secret information, but never to secret keys. Furthermore, England et al never discloses a secret signature key being distinctively associated with a sending station, and Examiner never contends otherwise. It is therefore respectfully requested that Examiner remove the rejection of Claim 6 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Claim 8

Claim 8 is dependant from Claim 1. As Claim 1 is allowable, so must be Claim 8. In addition, Claim 8 specifies that "said output data is encrypted with an encryption key unique

to said platform." 8/18/05 Response to 3/16/05 Office Action, P. 3. Furthermore, England et al never discloses an encryption key unique to the platform, and Examiner never contends otherwise. While Examiner contends that Rose discloses a decryption key unique to the platform, Examiner does not contend, and Rose does not disclose, output data encrypted with an encryption key unique to the platform. It is therefore respectfully requested that Examiner remove the rejection of Claim 8 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Claim 9

Claim 9 is dependant from Claim 8, which is in turn dependant form Claim 1. As Claim 1 is allowable, so must be Claim 9. In addition, Claim 9 specifies that "said output data is decrypted with an decryption key associated with said public encryption key." 8/18/05 Response to 3/16/05 Office Action, P. 3. England et al never discloses a decryption key that is associated with a public encryption key. It is therefore respectfully requested that Examiner remove the rejection of Claim 9 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Claim 10

Claim 10 is dependant from Claim 4, which is in turn dependant form Claim 1. As Claim 1 is allowable, so must be Claim 10. In addition, Claim 10 specifies that "wherein said output interface encrypts said output data when said output data includes at least a portion of data that has been authenticated by said operating system." 8/18/05 Response to 3/16/05 Office Action, P. 4. It is therefore respectfully requested that Examiner remove the rejection of Claim 10 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Claim 11

Claim 11 is dependant from Claim 1. As Claim 1 is allowable, so must be Claim 11. In addition, Claim 11 specifies that "wherein said operating system is capable of authenticating said input data by using a hash function." 8/18/05 Response to 3/16/05 Office Action, P. 4. While Examiner contends that "England discloses that the authentication procedure can be performed by a hash digest (Col. 9, lines 43-45)," Applicants respectfully disagree. Office Action (8/17/095), P. 8. That section of England et al, never once refers to any hash digest. Nor does any other portion of England et al refer to a hash digest. It is therefore respectfully requested that Examiner remove the rejection of Claim 11 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Claim 13

The Examiner objects to Claim 13 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose. However, Claim 13 is dependant from independent Claim 12. As Claim 12 is allowable, so must be Claim 13. In addition, because it is dependent from Claim 12 (to which Examiner objected to on the basis of anticipation), Claim 13 does not contain the limitation from Claim 1: "wherein **said operating system decrypts** said input data with a private **decryption key unique to that specific computer platform** to ensure that said input data is authorized for access on said specific computer platform alone." This is the only limitation which Examiner asserts is disclosed by Rose. Examiner has asserted that England et al discloses all other claim limitations. As such, this claim cannot be obvious over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose. Furthermore, since Claim 13 requires "a public key unique to

the receiving platform," and England et al never discloses such a public key, Claim 13 cannot be anticipated by England et al. It is therefore respectfully requested that Examiner remove the rejection of Claim 13 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Claim 15

The Examiner also objects to Claim 15 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose. However, Claim 15 is dependant from independent Claim 13, which is in turn dependant from independent Claim 12. As Claim 12 is allowable, so must be Claim 15. In addition, because it is dependent from Claim 12 (to which Examiner objected to on the basis of anticipation), Claim 15 does not contain the limitation from Claim 1: "wherein **said operating system decrypts** said input data with a private **decryption key unique to that specific computer platform** to ensure that said input data is authorized for access on said specific computer platform alone." This is the only limitation which Examiner asserts is disclosed by Rose. Examiner has asserted that England et al discloses all other claim limitations. As such, this claim cannot be obvious over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Examiner contends that "England discloses that the digital signature is created with a secret key (Col. 11. lines 6-17)." Office Action (8/17/05), P. 8. Applicant respectfully disagrees. As stated above, the portion of England cited by the examiner refers to public keys and to secret information, but never to secret keys. But even if Examiner is correct, Claim 15 requires that "said signature identification is provided through a signature creation algorithm and a secret key at said sending station **and through a signature verification algorithm and a**

public key at each receiving platform." 8/18/05 Response to 3/16/05 Office Action, P. 5 (emphasis added). England et al teaches that it is the content provider ("CP") that has the public key and not the receiving platform. Furthermore, England et al never discloses a signature creation algorithm, and Examiner never contends otherwise. Therefore, Claim 15 cannot be anticipated by England et al either. It is therefore respectfully requested that Examiner remove the rejection of Claim 15 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Claim 17

Claim 17 is a method claim similar to Claim 12 and requires:

> "authenticating an operating system to be loaded on a computer platform ... **to ensure that said operating system is approved to be loaded on that specific computer platform alone;**"

7/18/05 Response to 3/16/05 Office Action, P. 6 (emphasis added).

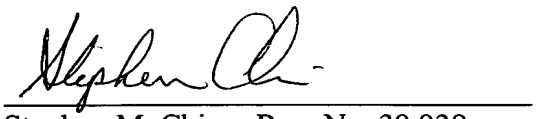
While examiner objects to this claim under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose, Claim 17 does not contain the one limitation for which Examiner uses Rose. As such, this claim cannot be obvious over England et al in view of Rose.

Furthermore, as discussed above in relation to Claim 12, the above Claim 17 limitation is not disclosed in England et al.

As such, Applicants respectfully assert that Examiner has failed to establish a prima facie case of obviousness of independent Claim 17 and corresponding claims 18-20 because they are dependant from Claim 17. Therefore, Applicants respectfully request that Examiner remove the rejection of claims 17-20 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Based upon the above remarks, Applicant respectfully requests reconsideration of this application and its early allowance. Should the Examiner feel that a telephone conference with Applicant's attorney would expedite the prosecution of this application, the Examiner is urged to contact him at the number indicated below.

Respectfully submitted,



SMC:JWT

Stephen M. Chin - Reg. No. 39,938
Reed Smith LLP
599 Lexington Avenue
New York, NY 10022
Tel. (212) 521-5400

500578.20076